MILLENNIUM CHALLENGE CORPORATION
UNITED STATES OF AMERICA

Notice Informing the Public of Improperly Stored Personally Identifiable Information (PII)

This notice is to inform the public that that personally identifiable information (PII) in the Millennium Challenge Corporation's (MCC) electronic network system of document files has been improperly stored. If you provided PII for yourself or someone else to MCC within the past five years, please read this notice carefully. PII for a number of individuals was stored on MCC's servers in folders that were not sufficiently secure. Accessible PII varied by individual, but included social security numbers, passport numbers, driver's license data, and date and/or place of birth – in most cases, not all of these data elements were accessible for a single individual. Each case is unique.

MCC has no evidence that any PII was misused. Access to MCC's network, even unsecured folders, is restricted to MCC personnel. MCC has no evidence that external agents have attempted to gain access to MCC information or that anyone inside MCC used the information in a way that would harm affected individuals. MCC's Office of Chief Information Officer (OCIO) discovered the improperly stored files on February 5, 2013 in response to an MCC help desk request. This situation developed over several years as MCC processes allowed some PII, including sensitive PII, to be accessible on the MCC network. Upon discovery of the improper handling of PII, the OCIO immediately and systematically moved all PII files to secure network folders with appropriate access controls.

In response to incidents like this and the increasing number of privacy incidents in the public and private sectors, MCC systems and practices are continuously monitored to enhance the security of personal and sensitive information. Steps are being taken to mitigate the loss of control of PII and to protect against and prevent further incidents.

Whenever sensitive PII is improperly stored, there is a risk for identity theft. While I view the risk of harm in this instance to be low, if you provided PII to MCC within the past 5 years, you may wish to consider taking the following actions as a precaution. First, consider contacting the three credit agencies listed below to place a fraud alert on your credit file to let creditors know to contact you before opening a new account in your name.

- Equifax: 1-888-766-0008; www.alerts.equifax.com
- Experian: 1-888-397-3742; www.experian.com/fraud/center
- TransUnion: 1-800-680-7289; www.transunion.com/personal-credit/credit-disputes-alerts-freezes.page

You may also request a free credit report annually from each agency. Some financial advisors recommend staggering your requests during a 12-month period as a good way to keep an eye on the accuracy and completeness of the information in your reports. When you receive your credit reports, review them carefully for accounts that you did not open or for inquiries from creditors that you did not initiate. Also, review your PII for accuracy – if you see anything that you do not recognize or understand, you should immediately call the credit agency.

If you find any suspicious activity on your credit reports, promptly file a report with your local police and the Federal Trade Commission. Suspicious activities could include the following:

- Inquiries from companies you have not contacted or done business with;
- Additional addresses, dates of birth, or names on your report that do not belong to you;
- Purchases or charges on your accounts you did not make;
- New accounts you did not open or changes to existing accounts you did not make;
- Bills that do not arrive as expected;
- Unexpected credit cards or account statements;
- Denials of credit for no apparent reason; and
- Calls or letters about purchases you did not make.

For additional information on identity theft, visit the Federal Trade Commission's identity theft Website at http://www.ftc.gov/idtheft/ or call the identity theft hotline at 1-877-438-4338. Please be cautious of any phone calls, e-mails, and other communications from individuals claiming to be from MCC or other official sources asking for your personal information or asking to verify such information. Legitimate requests for personal information from MCC will come directly from the MCC Security Office.

I apologize for this security lapse and for any inconvenience or concern this incident may cause you. I want to assure you that MCC's OCIO is working diligently to prevent a situation like this from occurring again. MCC takes its obligation to protect the security of PII very seriously. If you have questions regarding this letter, please contact the Chief Information Systems Security Officer and Deputy Chief Privacy Officer (mccciso@mcc.gov; mccprivacy@mcc.gov; or 202-521-3574).

Sincerely,

Chantale Wong
Vice President, Administration and Finance
Millennium Challenge Corporation